Thales nShield HSM と A10 Thunder の SSL アクセラレーション連携

堅牢な暗号鍵管理と保護によりアプリケーションのセキュリティを強化

課題：

SSL/TLS 通信のトラフィックが増加しアプリケーションの暗号処理が増加する一方で、ソフトウェア上で処理される暗号鍵は管理が煩雑で、暗号解読や攻撃により情報が漏えいする危険性もある

解決策：

SSL/TLS通信の暗号処理・鍵管理を耐タンパー性の高いハードウェア上で行うHardware Security Module（HSM）であるThales nShield HSMとA10 Thunder® CFW/ADCの連携により、アプリケーションのSSL/TLSアクセラレーション処理で利用される暗号鍵の堅牢な管理と保護を実現

メリット：

- HSM 利用によるセキュリティ強化
- FIPS140-2 Level3 などの基準を満たす高度なセキュリティの確保
- 高パフォーマンスでの暗号化処理
- Thales nShield HSM の負荷分散による高可用性と拡張性

A10 Networks® と Thales は、増加する暗号化通信のセキュリティ強化に関する連携を進めています。A10 Thunder CFW/ADC シリーズがサーバーの SSL/TLS アクセラレーションを行う際に利用される暗号鍵の管理と保護、および暗号化処理を Thales nShield HSM のハードウェア上で行うことで、高度なセキュリティを確保すると同時に、高パフォーマンスでの処理を実現します。このソリューションにより、FIPS などの高度なセキュリティ基準を満たしたセキュアで高速なアプリケーションを提供できます。

課題

SSL/TLS 通信の増大と暗号鍵管理の脆弱性

セキュリティとプライバシーの懸念により多くのアプリケーションで SSL/TLS 通信の適用が進んでおり、特に高度なセキュリティを要求されるオンライン取引においてはデファクトスタンダードとして利用されています。また、今日では多くの有名な Web サイトも全ての Web リクエストとレスポンスを暗号化しており、2016 年までには 2/3 のインターネットトラフィックが暗号化されると予測されています。アプリケーションのパフォーマンスを落とさずに、SSL/TLS 通信の増大に伴い増加する暗号処理に対応するには多くの演算リソースが必要になり、多くのサーバーでの処理が必要になりますが、これにより暗号鍵の管理は煩雑化します。

ソフトウェアによる暗号処理は、高品質な乱数を発生できないために暗号を解読される可能性があります。また、サーバー上に保管された暗号鍵は、サーバーへの攻撃や暗号鍵をメモリ上に展開する際の盗聴などにより漏えいする危険性があります。暗号鍵が漏えいすると SSL/TLS 通信が解読されてしまうため、機密情報の流出やクレジットカードの偽造などに繋がります。このような事態を防ぐためには、安全な環境での暗号鍵の保護が重要になります

A10 Thunder CFW/ADC と Thales nShield HSM の連携

ハードウェアベースでの鍵管理と保護

Thales の提供する Hardware Security Module（HSM）である nShield HSM を利用することで、SSL/TLS 通信の暗号処理や鍵管理を耐タンパー性の高いハードウェア上で行うことができます。その結果、暗号鍵を安全に管理・保護することが可能になると共に、暗号化処理や署名処理のオフロードも可能になります。Thales nShield HSM はマルチクライアント接続・高可用性を意識した製品設計になっており、多様な暗号アルゴリズムに対応しており、FIPS や CC などの政府機関が要求するセキュリティ認定を取得しています。鍵のアクセスログ等により、監査や追跡調査の負担も軽減します。

SSL/TLS アクセラレーションと HSM の連携

A10 ネットワークスの Thunder CFW/ADC シリーズはアプリケーション配信の高速化機能として、HTTP/HTTPS や FIX を含む多様なプロトコルに対応したサーバー負荷分散機能に加え、サーバーの SSL/TLS 通信に関わる処理をオフロードする SSL/TLS アクセラレーションの機能を持っています。専用のハードウェアによる処理を行うことで、アプリケーションサーバーの CPU 負荷を大きく軽減することができるとともに、暗号鍵の管理を一元的に行うことで運用負荷も軽減します。

Thales nShield HSMとの連携により、A10 Thunder のSSL/TLSアクセラレーションで利用される暗号鍵の堅牢な管理と保護が可能になります。（図1）。この連携では、暗号鍵はThales nShield HSMのハードウェア内に保管されており、暗号化処理や署名処理をHSM上で実施することで、暗号鍵の堅牢な管理と保護、および暗号処理の高速化が実現されます。

特長とメリット

Thales nShield HSM とA10 Thunder CFW/ADCとの連携には、以下の特長とメリットがあります。

- **セキュリティ強化の実現：**HSMを利用することにより暗号鍵をA10 Thunderから物理的に分離して管理
- **セキュリティ基準への準拠：**FIPS140-2 Level3などの基準を満たす高度なセキュリティの確保
- **高パフォーマンス暗号化処理：**Thales nShield HSMとA10 Thunderが連携したSSL/TLSアクセラレーションにより高いパフォーマンスを実現
- **高可用性と拡張性：**Thales nShield HSMをA10 Thunder CFW/ADCで負荷分散することにより高い可用性と拡張性を実現

また、A10 Thunder CFW/ADCをアプリケーションサーバーの負荷分散およびSSL/TLSアクセラレーションに用いることで、TCPコネクションリユースなどのアプリケーション配信高速化機能や、DDoS防御機能、Web Application Firewall（WAF）、L4ステートフルファイアウォールなどによるセキュリティ機能、NAT機能、グローバル負荷分散などの機能が利用可能になり、セキュアで高速かつ可用性の高いアプリケーション利用が実現できます。

結論

オンライン取引などの高いセキュリティが求められるアプリケーションにおいてはSSL/TLS通信で利用される暗号鍵の堅牢な管理と暗号処理の高速化が重要な課題となります。高速化と負荷分散を実現するA10 Thunder CFW/ADCのSSL/TLSアクセラレーションと、暗号鍵の堅牢な管理と保護を実現するThales nShield HSMの連携により、セキュリティ強化と可用性の向上を両立することができます。これにより、FIPSなどの高度なセキュリティ基準を満たした、セキュアなアプリケーション利用が実現されます。

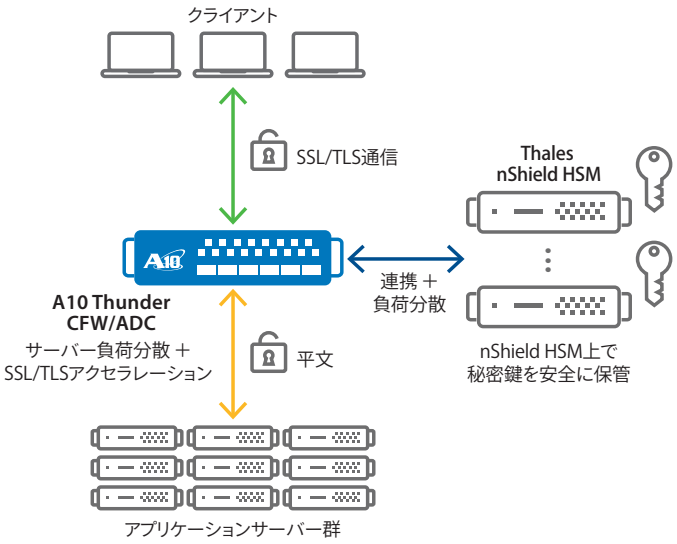

図1: Thales nShield HSMとA10 Thunder CFW/ADCの連携

タレス e-Security について

タレス e-Securityは、デジタルトラスト管理とデータ保護ソリューションを提供する世界規模のトッププロバイダです。機密性の高いアプリケーションと情報を保護してきました。Thales e-Securityが提供するソリューションは、ソフトウエアベースの暗号、デジタル署名、管理機能とハードウェアのセキュリティを組み合わせることにより、認証や機密保護に関連する課題を解決します。つながる世界の進化の中でもタレス e-Securityのソリューションにより、標的型攻撃を阻止することが可能です。また、クラウドコンピューティング、仮想化、職場でのコンシューマデバイスの利用、モビリティの向上、ビッグデータなどでもたらされた新しい課題も解決でき、機密情報の漏洩リスクを最小化することが可能です。タレス e-Securityは、米国、イギリス、香港に地域本部を持っており、世界規模でのサービス提供が可能です。www.thales-esecurity.com。

A10 Networks / A10 ネットワークス株式会社について

A10 Networks（NYSE: ATEN）はアプリケーションネットワーキング分野におけるリーダーとして、高性能なアプリケーションネットワーキングソリューション群を提供しています。世界中で数千社にのぼる大企業やサービスプロバイダー、大規模Webプロバイダーといったお客様のデータセンターに導入され、アプリケーションとネットワークを高速化し安全性を確保しています。A10 Networksは2004年に設立されました。米国カリフォルニア州サンノゼに本拠地を置き、世界各国の拠点からお客様をサポートしています。

A10ネットワークス株式会社はA10 Networksの日本子会社であり、お客様の意見や要望を積極的に取り入れ、革新的なアプリケーションネットワーキングソリューションをご提供することを使命としています。
詳しくはホームページをご覧ください。
www.a10networks.co.jp
Facebook：http://www.facebook.com/A10networksjapan

A10ネットワークス株式会社
〒105-0001
東京都港区虎ノ門4-3-20
神谷町MTビル16階
TEL：03-5777-1995
FAX: 03-5777-1997
jinfo@a10networks.com
www.a10networks.co.jp

海外拠点

北米（A10 Networks本社）
sales@a10networks.com
ヨーロッパ
emea_sales@a10networks.com
南米
latam_sales@a10networks.com
中国
china_sales@a10networks.com
香港
HongKong@a10networks.com
台湾
taiwan@a10networks.com
韓国
korea@a10networks.com
南アジア
SouthAsia@a10networks.com
オーストラリア/ニュージーランド
anz_sales@a10networks.com

お客様のビジネスを強化するA10のアプリケーションサービスゲートウェイ、Thunderの詳細は、A10ネットワークスのWebサイト**www.a10networks.co.jp**をご覧になるか、A10の営業担当者にご連絡ください。

Part Number: A10-SB-90013-JA-01
Aug 2016